

Express Mail Label No. _____	Dated: _____
------------------------------	--------------

Docket No.: 20046/0201102-US0
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Wieland Fischer et al.

Application No.: 10/825,625

Confirmation No.: 7860

Filed: April 15, 2004

Art Unit: 2131

For: METHOD AND APPARATUS FOR
PROTECTING AN EXPONENTIATION
CALCULATION BY MEANS OF THE
CHINESE REMAINDER THEOREM (CRT)

Examiner: Not Yet Assigned

CLAIM FOR PRIORITY AND SUBMISSION OF DOCUMENTS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:


Applicant hereby claims priority under 35 U.S.C. 119 based on the following prior foreign applications filed in the following foreign countries on the dates indicated:

<u>Country</u>	<u>Application No.</u>	<u>Date</u>
Germany	101 51 139.6	October 17, 2001
Germany	101 62 584.7	December 19, 2001

In support of this claim, a certified copy of each said original foreign application is filed herewith.

Dated: August 24, 2004

Respectfully submitted,

By  *Laura C. Brutman*
Laura C. Brutman

Registration No.: 38,395
DARBY & DARBY P.C.
P.O. Box 5257
New York, New York 10150-5257
(212) 527-7700
(212) 753-6237 (Fax)
Attorneys/Agents For Applicant

BUNDESREPUBLIK DEUTSCHLAND



Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 101 51 139.6

Anmeldetag: 17. Oktober 2001

Anmelder/Inhaber: Infineon Technologies AG, 81669 München/DE

Bezeichnung: Verbesserte Gegenmaßnahme gegen eine differenzielle Fehleranalyse für RSA mit CRT

IPC: H 04 L 9/30

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 19. April 2004
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Faust

PATENTANWÄLTE

European Patent Attorneys
European Trademark Attorneys

Patentanwälte · Postfach 710867 · 81458 München

Infineon Technologies AG

St.-Martin-Str. 53

81669 München

Fritz Schoppe, Dipl.-Ing.
Tankred Zimmermann, Dipl.-Ing.
Ferdinand Stöckeler, Dipl.-Ing.
Franz Zinkler, Dipl.-Ing.

Telefon/Telephone 089/790445-0
Telefax/Facsimile 089/790 22 15
Telefax/Facsimile 089/74996977

e-mail: szsz_iplaw@t-online.de

**Verbesserte Gegenmaßnahme gegen eine differentielle
Fehleranalyse für RSA mit CRT**

1. Welches technische Problem soll durch Ihre Erfindung gelöst werden?

Differential Faults Attacks wie sie von Boneh et alii im Journal of Cryptology auf das RSA (mit/ohne CRT) Verfahren vorgestellt werden, werden in der Praxis meist durch Software Gegenmaßnahmen, wie etwa dem US Patent 5991415 von A. Shamir, abgefangen.

Diese Gegenmaßnahmen sind aber oftmals nicht erfolgreich gegen eine bisher nicht betrachtete Art von häufig vorkommenden Fehlern, und damit ungenügend.

2. Wie wurde dieses Problem bisher gelöst?

Gegenrechnen mit dem öffentlichen Exponenten e , womit die Identität $(M^d)^e = M \bmod N$ festgestellt werden soll.

Allerdings ist dieses e in den üblichen Protokollen (ZKA-lib) nicht explizit verfügbar, und müßte deshalb aufwendig berechnet werden. Hinzu kommt, daß das Gegenrechnen i.a. sehr aufwendig sein kann.

3. In welcher Weise löst Ihre Erfindung das angegebene technische Problem (geben Sie Vorteile an)?

Die vorgeschlagene Methode erkennt die obigen Fehler und vermeidet aufwendiges Rechnen bzgl. e .

4. Worin liegt der erfinderische Schritt?

Der erfinderische Schritt liegt in der genauen Analyse der möglichen Fehlerquellen, die ein Angreifer induzieren kann und speziellen Überprüfungen hinsichtlich möglicher Fehler.

5. Ausführungsbeispiel[e] der Erfindung.

Input: Message m ,
Primzahlen p und q ,
Exponenten $dp := d \bmod (p-1)$ und $dq := d \bmod (q-1)$,
 $qinv := (q \bmod p)^{-1}$

- Wähle kleine Primzahl t (ca. 16 Bit, nicht F_4)
- $p' := p * t$, $dp' := dp + \text{random} * (p-1)$
- $sp' := m^{dp'} \bmod p'$
- if NOT($(p' \bmod p = 0)$ AND $(dp' \bmod (p-1) = dp)$) return ERROR
- $q' := q * t$, $dq' := dq + \text{random} * (q-1)$
- $sq' := m^{dq'} \bmod q'$
- if NOT($(q' \bmod q = 0)$ AND $(dq' \bmod (q-1) = dq)$) return ERROR
- $spt := sp' \bmod t$, $dpt := dp' \bmod (t-1)$
- $sqt := sq' \bmod t$, $dqt := dq' \bmod (t-1)$
- if NOT($spt^{dqt} = sqt^{dpt} \bmod t$) return ERROR
- $sp := sp' \bmod p$, $sq := sq' \bmod q$
- $s := sq + ((sp - sq) * qinv \bmod p) * q$
- if ($(s \bmod p = sp)$ AND $(s \bmod q = sq)$)
 return s
- else
 return ERROR

Output: $m^d \bmod (p*q)$ oder error message